

CLAIMS

I claim:

- 5           1. A system comprising:  
          /a security management system comprising:  
              a network security feedback and control  
              system wherein said security feedback and  
              control system receives a plurality of  
10           normalized events and issues at least one  
              normalized command in response to a  
              predefined event in said plurality of  
              normalized events.
- 15           2. The system of Claim 1 wherein said network  
security feedback and control system comprises:  
              a feedback and control manager wherein said  
              feedback and control manager processes said at  
              least one normalized event and generates said at  
20           least one normalized command.
3. The security management system of Claim 2  
              wherein said feedback and control manager includes at  
              least one rules engine wherein said rules engine  
25           includes a rule having a condition object that uses  
              information from said at least one normalized event.
4. The system of Claim 1 further comprising:  
              a managed node coupled to said security  
30           management system.
5. The system of Claim 4 wherein said managed  
node further comprises:  
              a security management agent executing on said  
35           managed node.

6. The system of Claim 5 further comprising:  
at least one managed product coupled to said  
security management agent wherein said at least  
one managed product forwards at least one of said  
normalized events to said security management  
agent and receives normalized commands from said  
security management agent.
7. The system of Claim 1 further comprising:  
a security management agent coupled to said  
network security feedback and control system  
wherein said security management agent collects  
normalizes events and forwards said normalized  
events to said security management system.
8. The system of Claim 7 further comprising:  
at least one managed product coupled to said  
security management agent wherein said at least  
one managed product transfers at least one  
normalized event to said security management  
agent.
9. A system comprising:  
an event subscription filter;  
a feedback and control manager coupled to  
said event subscription filter.
10. The system of Claim 9 further comprising:  
a knowledge database coupled to said feedback  
and control manager.
11. The system of Claim 9 further comprising:  
a directory coupled to said feedback and  
control manager.
12. The system of Claim 11 further comprising:

a configuration adapter connected between said feedback and control manager and said directory.

5           13. The system of Claim 9 wherein said feedback and control system further comprises a rules engine coupled to said event subscription filter.

10           14. The system of Claim 9 further comprising:  
a security management agent coupled to said event subscription filter.

15           15. The system of Claim 14 further comprising:  
at least one managed product coupled to said security management agent

20           16. A method comprising:  
receiving events from managed products by a network security feedback and control system; and  
using information in said events by said network feedback and control system in dynamically implementing a predefined security policy.

25           17. A computer-program product comprising a computer-readable medium containing computer program code for a method comprising:

30           receiving events from managed products by a network security feedback and control system; and  
using information in said events by said network feedback and control system in dynamically implementing a predefined security policy.

18. A structure comprising:

means for receiving events from managed products by a network security feedback and control system; and

5 means using information in said events by said network feedback and control system in dynamically implementing a predefined security policy.

19. A method comprising:  
10 collecting events, from a plurality of managed products in a first tier, in a second tier object;  
forwarding said events to a third tier object; and  
15 routing said events to an event sink in said third tier object for processing.

20. The method of Claim 19 wherein said event sink comprises a security feedback and control system.  
20

21. The method of Claim 19 wherein said second tier object comprises a security management agent.

22. The method of Claim 19 wherein said third  
25 tier object comprises a security management server.

23. A computer-program product comprising a computer-readable medium containing computer program code for a method comprising:  
30 collecting events, from a plurality of managed products in a first tier, in a second tier object;  
forwarding said events to a third tier object; and  
35 routing said events to an event sink in said third tier object for processing.

24. A structure comprising:  
means for collecting events, from a plurality  
of managed products in a first tier, in a second  
5 tier object;  
means for forwarding said events to a third  
tier object; and  
means for routing said events to an event  
sink in said third tier object for processing.  
10
25. A method comprising:  
collecting security events having predefined  
structures from a plurality of managed products by  
a security management agent;  
15 forwarding said security events to a security  
management system upon a connection to said  
security management system being available; and  
forwarding said security events to a network  
management application upon said connection to  
20 said security management system being unavailable.
26. A computer-program product comprising a  
computer-readable medium containing computer program  
code for a method comprising:  
25 collecting security events having predefined  
structures from a plurality of managed products by  
a security management agent;  
forwarding said security events to a security  
management system upon a connection to said  
30 security management system being available; and  
forwarding said security events to a network  
management application upon said connection to  
said security management system being unavailable.
- 35 27. A structure comprising:

means for collecting security events having predefined structures from a plurality of managed products by a security management agent;

5 means for forwarding said security events to a security management system upon a connection to said security management system being available; and

10 means for forwarding said security events to a network management application upon said connection to said security management system being unavailable.

28. A method comprising:

15 issuing a command for a security managed product wherein said issuing said command is performed on a first computer system;

20 pinging a security management agent following said issuing said command wherein said security management agent is executing on a second computer system coupled to said first computer system; and

downloading said command securely by said security management agent following said pinging said security management agent.

25 29. A computer-program product comprising a computer-readable medium containing computer program code for a method comprising:

30 issuing a command for a security managed product wherein said issuing said command is performed on a first computer system;

pinging a security management agent following said issuing said command wherein said security management agent is executing on a second computer system coupled to said first computer system; and

downloading said command securely by said security management agent following said pinging said security management agent.

5        30. A structure comprising:

means for issuing a command for a security managed product wherein said issuing said command is performed on a first computer system;

10        means for pinging a security management agent following said issuing said command wherein said security management agent is executing on a second computer system coupled to said first computer system; and

15        means for downloading said command securely by said security management agent following said pinging said security management agent.

31. A method comprising:

20        specifying a plurality of hierarchical security event structures for use by heterogeneous security managed products; and

25        including in said plurality of hierarchical event structures information for security management of said heterogeneous security managed products.

32. The method of Claim wherein 31 said plurality of hierarchical security event structures includes a security base event structure.

30

33. The method of Claim 32 wherein said security base event structure includes an event identifier field.

34. The method of Claim 32 wherein said security base event structure includes a software feature identifier field.

5        35. The method of Claim 32 wherein said security base event structure includes a severity field.

36. The method of Claim 32 wherein said security base event structure includes a category field.

10

37. A computer-program product comprising a computer-readable medium containing computer program code for a method comprising:

15        specifying a plurality of hierarchical security event structures for use by heterogeneous security managed products; and

      including in said plurality of hierarchical event structures information for security management of said heterogeneous security managed products.

20

38. A structure comprising:

25        means for specifying a plurality of hierarchical security event structures for use by heterogeneous security managed products; and

      means for including in said plurality of hierarchical event structures information for security management of said heterogeneous security managed products.

30

39. A memory structure comprising:

      a security event structure including:

          an event identifier field;

          an event class identifier field; and

35        a category field.



40. The memory structure of Claim 39 wherein said security event structure further comprises:  
a severity field.

5           41. The memory structure of Claim 39 wherein said security event structure further comprises:  
a software feature identifier field.

42. The memory structure of Claim 39 wherein said  
10 security event structure is a base event structure.

43. The memory structure of Claim 39 wherein said security event structure is an application update event structure.  
15

44. The memory structure of Claim 39 wherein said security event structure is a configuration update event structure.

20           45. The memory structure of Claim 39 wherein said security event structure is a definition update event structure.

46. The memory structure of Claim 39 wherein said  
25 security event structure is a network event structure.

47. The memory structure of Claim 39 wherein said security event structure is an instruction event structure.  
30

48. The memory structure of Claim 39 wherein said security event structure is a host instruction event structure.

49. The memory structure of Claim 39 wherein said security event structure is a network instruction event structure.

5 50. The memory structure of Claim 39 wherein said security event structure is a network firewall event structure.

51. The memory structure of Claim 39 wherein said  
10 security event structure is a firewall connection statistics event structure.

52. The memory structure of Claim 39 wherein  
15 said security event structure is a data scan event structure.

53. The memory structure of Claim 39 wherein said  
20 security event structure is a data incident event structure.

54. The memory structure of Claim 39 wherein said security event structure is a data virus incident event structure.

25 55. The memory structure of Claim 39 wherein said security event structure is an advisory malware event structure.

56. The memory structure of Claim 39 wherein said  
30 security event structure is an malware activity event structure.

57. A method comprising:  
collecting security events having predefined  
35 structures from a plurality of managed products by a security management agent; and

queuing said security events by said security management agent.

5        58. The method of Claim 57 further comprising:  
transferring queued security events upon a predefined criterion being true.

10       59. The method of Claim 58 wherein said predefined criterion comprises a queue flush time.

60. The method of Claim 58 wherein said predefined criterion comprises a queue flush size.

15       61. The method of Claim 58 wherein said predefined criterion comprises a queue flush count.

20       62. The method of Claim 57 wherein said queuing said security events further comprises:  
queuing only security events not marked as alert events.

25       63. The method of Claim 57 wherein said queuing said security events further comprises:  
queuing all of said security events in a single queue.

30       64. The method of Claim 57 wherein said queuing said security events further comprises:  
queuing said security events in a plurality of queues.

65. A computer-program product comprising a computer-readable medium containing computer program code for a method comprising:

collecting security events having predefined  
structures from a plurality of managed products by  
a security management agent; and

5           queuing said security events by said security  
management agent.

66. A structure comprising:

10           means for collecting security events having  
predefined structures from a plurality of managed  
products by a security management agent; and

          means for queuing said security events by  
said security management agent.

67. A method comprising:

15           collecting security events having predefined  
structures from a plurality of managed products by  
a security management agent;

          queuing only security events of said security  
that are not alert events

20           transferring said alert events to an output  
buffer without queuing said alert events.